#4

Please type a plus sign (+) inside this box → [+]

PTO/SB/21 (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/816,684
Filing Date	03/26/2001
First Named Inventor	SUDIA
Group Art Unit	2132
Examiner Name	
Total Number of Pages in This Submission	
Attorney Docket Number	10624.0004 D1

ENCLOSURES *(check all that apply)*

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment / Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [X] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Assignment Papers *(for an Application)*
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) *(please identify below)*:

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	STEPTOE & JOHNSON LLP Stuart T.F. Huang
Signature	Stuart T.F. Huang
Date	27 Aug 01

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, Washington, DC 20231 on this date: [ ]

Typed or printed name			
Signature		Date	

PATENT APPLICATION
Atty. Dkt.: 10624.0004 D1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Applicant: SUDIA

Group Art Unit: 2132

Serial No.: 09/816,684

Filed: 03/26/2001

For: MULTI-STEP DIGITAL SIGNATURE METHOD AND SYSTEM

INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

Attached are copies of forms PTO-1449 and PTO-892 listing all of the documents cited by Applicant and the USPTO in the parent application Serial No. 09/161,741, filed September 29, 1998, now U.S. Patent No. 6,209,091, relied upon under 35 U.S.C. § 120 and referenced in the first sentence of the specification, as amended by the Preliminary Amendment, filed March 26, 2001. Per Rule 98(d), Applicant is not required to provide copies of these documents.

It is respectfully requested that the references be expressly considered during the prosecution of this application and made of record herein and among the "References Cited" on any patent to issue therefrom. Consideration of the foregoing and enclosures is earnestly solicited.

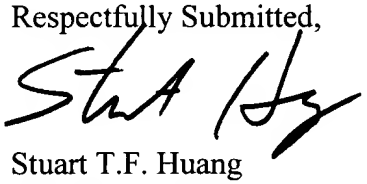
This Information Disclosure Statement is intended to be in full compliance with the Rules, but should the Examiner find any part of its required content to have been omitted, prompt notice to that effect is earnestly solicited, along with additional time under Rule 97(f), to enable Applicant to comply fully.

In submitting this Information Disclosure Statement, Applicant does not waive the right to challenge the prior status of any of the documents cited therein.

It is Applicant's belief that no fee for this Information Disclosure Statement is necessary as it is being filed prior to the first Office Action in accordance with Rule 97(b)(3). If it is determined, however, that a fee for filing this Information Disclosure Statement is required, the Commissioner is hereby authorized to charge any required fees to Deposit Account No. 19-4293 (Order No. 10624.0004 D1).

Date: August 23, 2001

Respectfully Submitted,



Stuart T.F. Huang
Reg. No. 34,184

STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, NW
Washington, D.C. 20036-1795

Tel.: (202) 429-3000
Fax: (202) 429-3902

Date Mailed: January 28, 1999

FORM 1449 (S&J Version)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Docket No.: 10624.0004	
Applicant: SUDIA et al	
Application No.: 09/161,741	
Filing Date: September 29, 1998	
Examiner: G. Baron Jr.	Group Art Unit: 3642

U.S. PATENT DOCUMENTS

Examiner's Initials*	Document No.	Date MM/YYYY	Inventor	Class	Subclass	Filing Date If Appropriate
	5,224,163	6/1993	Gasser et al.	380	30	
	5,276,737	1/1994	Micali	380	30	
	5,481,613	1/1996	Ford et al.	380	30	
	5,005,200	4/1991	Fischer	380	30	
	5,164,988	11/1992	Matyas et al.	380	30X	

FOREIGN PATENT DOCUMENTS

Examiner's Initials*	Document No.	Date MM/YYYY	Country	Class	Subclass	Translation Yes	Translation No

OTHER DOCUMENTS

Examiner's Initials*	Include author, title of article, title of item (book, journal, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	DESMEDT et al., "Shared generation of authenticators and signatures", Lecture Notes in Computer Science 576, Advances in Cryptology, CRYPTO '91, 1991, pp . 457-469
	LI et al., "Remark on the Threshold RSA Signature Scheme", Lecture Notes in Computer Science 773, Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, August 1993, pp.413-419
	PEDERSEN, "A Threshold Cryptosystem Without a Trusted Party", Lecture Notes in Computer Science 547, Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, April 1991, pp. 522-526
	CHANG et al., "A New Generalized Group-Oriented Cryptoscheme Without Trusted Centers", IEEE Journal on Selected Areas of Communications, June 1993, pp. 725-729, Vol. 11, No. 5
	FRANKEL et al., "Non-existence of homomorphic general sharing schemes for some key spaces, pp. 549-557
	PEDERSEN, "Distributed Provers with Applications to Undeniable Signatures", Aarhus University, Computer Science Department, Ny Munkegade, DK-8000 Arhus C, Denmark, pp. 221-242
	REITER et al., "How to Securely Replicate Services", pp. 987-1009
	DESMEDT et al., "Homorphic Zero-Knowledge Threshold Schemes Over Any Finite Abelian Group", SIAM J. DISC MATH., Vol. 7, No. 4, pp. 667-679, November 1994
	Y. FRANKEL, "A practical protocol for large group oriented networks", Advances in Cryptology, Proc. of Eurocrypt '89, (Lecture Notes in Computer Science 434) (1990), J.-J. Quisquater and J. Vandewalle, Eds. Springer-Verlag, pp. 56-61
	Y. DESMEDT et al., "Shared generation of authenticators and signatures", Advances in Cryptology, Crypto '91, Proceedings (Lecture Notes in Computer Science 576)(1992), J. Feigenbaum, Ed. Springer-Verlag, pp. 457-469
	A. SHAMIR, "How to share a secret", Commun. ACM 22 (1979) 612-613
	A. DE SANTIS et al., "How to share a function securely"
	Y. DESMEDT, "Threshold Cryptosystems"
	Y. DESMEDT, "Threshold Cryptography", July/August 1994
	HAM, "Group-oriented (t,n) threshold digital signature scheme and digital multisignature", IEE Proc. Comput. Digit. Tech. Vol. 141, No. 5, September 1994, pp. 307-313

Examiner's Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM 1449 (S&J Version)	Docket No.: 10624.0004	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant: SUDIA et al	
	Application No.: 09/161,741	
	Filing Date: herewith	
	Examiner: G. Baron Jr.	Group Art Unit: 3642

U.S. PATENT DOCUMENTS

Examiner's Initials*	Document No.	Date MM/YYYY	Inventor	Class	Subclass	Filing Date If Appropriate

FOREIGN PATENT DOCUMENTS

Examiner's Initials*	Document No.	Date MM/YYYY	Country	Class	Subclass	Translation Yes	Translation No

OTHER DOCUMENTS

Examiner's Initials*	Include author, title of article, title of item (book, journal, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	C. BOYD, "Some Applications of Multiple Key Ciphers", undated
	"Threshold Hashing and Signing", Extended Abstract, undated
	R.A. CROFT et al., "Public-Key Cryptography and Re-Usable Shared Secrets"
	C. BOYD, "Digital Multisignatures", Cryptography and Coding
	Y. FRANKEL, "A Practical Protocol for Large Group Oriented Networks"
	B. BLAKLEY et al., "Threshold Schemes With Disenrollment"

Examiner's Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.